

UNITED STATES DISTRICT COURT

for the

In the Matter of the Search of
*(Briefly describe the property to be searched
 or identify the person by name and address)*

See Attachment A

17 MAG 4152
 Case No.

APPLICATION FOR A SEARCH AND SEIZURE WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Southern District of New York, there is now concealed *(identify the person or describe the property to be seized)*:

See Attached Affidavit and its Attachment A

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section(s)

Offense Description(s)

18 USC 2339B, 2339D/371, material support or resources to designated foreign terrorist organizations (FTOs);
 924, 1001, 1425 receipt of military-type training from FTOs; firearms offenses related to crimes of
 violence; false statements; naturalization fraud

The application is based on these facts:

See Attached Affidavit and its Attachment A

- ☒ Continued on the attached sheet.
☐ Delayed notice of 30 days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

(Signature)
 Applicant's signature

Joseph T. Costello, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 5-31-17

City and state: New York, NY

(Signature)
 Judge's signature

Hon. Katharine H. Parker, USMJ, SDNY

Printed name and title

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF
THE PREMISES KNOWN AND
DESCRIBED AS 183 WEST 238
STREET, APARTMENT 51W, BRONX,
NEW YORK 10463.

TO BE FILED UNDER SEAL

**Agent Affidavit in Support of
Application for Search and Seizure
Warrant**

**Affidavit in Support of Application Pursuant to Rule 41
For a Warrant to Search and Seize**

SOUTHERN DISTRICT OF NEW YORK) ss.:

JOSEPH T. COSTELLO, being duly sworn, deposes and states:

I. Introduction

1. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") for approximately three years. Prior to joining the FBI, I served as a Special Agent with the U.S. Department of State, Diplomatic Security Service, for approximately five years. For the last approximately two years, I have been assigned to the FBI's New York Joint Terrorism Task Force ("JTTF"). During this time period, I have participated in numerous investigations of unlawful activity, principally national security related matters and crimes relating to immigration fraud. During the course of these investigations, I have conducted or participated in surveillance, the introduction and debriefings of informants, and the execution of search warrants. Through my training, education, and experience, I have become familiar with various terrorist organizations, as well as the manner in which terrorists are recruited, receive training, and operate, and some of the methods that are used to conceal evidence of participation in such illegal activity. I have received

training in the use of computer technology by terrorist networks and have participated in investigations involving the use of computers, the Internet, and social media by terrorists and terrorist organizations. Through my training and experience, I have become familiar with some of the ways in which terrorist groups use the Internet, including social media and email, to promote their activities, recruit new members, and issue threats, and I have also participated in the execution of search warrants involving electronic evidence.

II. The Subject Premises

2. I respectfully submit this Affidavit in support of an application for a warrant to search the entire premises, including all closed and locked containers, closets, and rooms at the premises located at 183 West 238 Street, Apartment 51W, Bronx, New York 10463 (the "Subject Premises"), which is an apartment in a multi-story apartment building that appears from the outside as follows:



3. For the reasons set forth below, I respectfully submit that there is probable cause to believe that the Subject Premises contain evidence, fruits, and instrumentalities of (i) Title 18, United States Code, Section 2339B (providing and conspiracy to provide material support or

resources to designated foreign terrorist organizations); (ii) Title 18, United States Code, Sections 2339D and 371 (receipt of, and conspiracy to receive, military-type training from designated foreign terrorist organizations); (iii) Title 18, United States Code, Section 924 (firearms offenses related to crimes of violence); (iv) Title 18, United States Code, Section 1001 (making false statements or omissions in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States); and (v) Title 18, United States Code, Section 1425 (procurement of citizenship or naturalization unlawfully) (the "Subject Offenses"), committed by Ali Kourani, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel" ("Kourani"), and others known and unknown.

4. I am familiar with the information contained in this Affidavit based on my own personal participation in the investigation, my review of documents, conversations I have had with others about this matter, and my training and experience. Because this Affidavit is being submitted for the limited purpose of establishing probable cause to search the Subject Premises, I have not included herein the details of every aspect of the investigation. Where actions, conversations and statements of others, and the contents of documents are related herein, they are related in substance and in part, except where otherwise indicated.

III. Facts Establishing Probable Cause

A. Hizballah and the Islamic Jihad Organization (IJO)

5. Based on my training, experience, and participation in this and related investigations, I am aware of the following:

a. Hizballah (or Hezbollah)—which is Arabic for “Party of God”—is based in Lebanon. Hizballah was founded in the early 1980s with support from Iran, after the 1982 Israeli invasion of Lebanon. Hizballah’s mission includes establishing a fundamentalist Islamic state in Lebanon.

b. The Islamic Jihad Organization (“IJO”), which is also known as the External Security Organization (“ESO”) and “910,” is a component of Hizballah responsible for the planning and coordination of attacks by Hizballah outside Lebanon.

c. Since its formation, Hizballah has been responsible for numerous terrorist attacks that have killed hundreds, including the 1983 bombing of the United States Marine barracks in Lebanon, which killed 241 Marines; the 1983 bombing of the United States Embassy in Beirut, which killed 24 people; the 1985 hijacking of TWA flight 847, which killed at least one U.S. citizen; the 1992 bombing of the Israeli Embassy in Argentina, which killed 29 people; and the 1994 bombing of a Jewish cultural center in Buenos Aires, which killed 95 people.

d. In 1995, the United States Department of State designated Hizballah as a Foreign Terrorist Organization, pursuant to section 219 of the Immigration and Nationality Act, and it remains so designated today.

e. In 2001, pursuant to Executive Order 13,224, the United States named Hizballah as a Specially Designated Global Terrorist entity.

f. In July and August 2006, Hizballah and Israel engaged in armed conflict, resulting in numerous casualties, after an incident on or about July 12, 2006 when Hizballah attacked Israeli Defense Force personnel. A ceasefire brokered by the United Nations went into effect on August 14, 2006.

g. In January 2012, a Hizballah operative named Hussein Atris was detained in Thailand as he tried to board a flight at Bangkok Airport. Atris subsequently led law enforcement personnel to a cache of nearly 10,000 pounds of urea-based fertilizer and 10 gallons of ammonium nitrate (stored in First Aid ice packs)—chemicals that I know, based on my training and experience, can be used to construct explosives—stored in a commercial building near Bangkok.

h. In July 2012, a suicide bomber detonated explosives on a bus transporting Israeli tourists in the vicinity of an airport in Burgas, Bulgaria. Six people were killed and 32 others were injured. Bulgarian authorities subsequently made public statements relating to evidence linking the attack to Hizballah.

i. In May 2015, a Hizballah operative named Hussein Bassam Abdallah was arrested in Cyprus after Cypriot authorities seized from an apartment rented by Abdallah approximately 8.2 tons of ammonium nitrate, at least some of which was stored in First Aid ice packs manufactured by the same company, and with the same lot number, as the First Aid ice packs with ammonium nitrate that were seized in Thailand in January 2012. *See*, paragraph 5(g), *supra*. Abdallah was subsequently convicted in Cyprus of charges relating to surveillance of Israeli tourist targets.

B. Ali Kourani

6. Based on my review of documents and information maintained by federal and state authorities in the United States, I am aware of the following:

- a. Ali Kourani (“Kourani”) was born in Bint Jubayl, Lebanon in 1984.
- b. In 2003, Kourani lawfully entered the United States from Cyprus.

c. In approximately August 2008, Kourani submitted an application for naturalization in the United States (the “Naturalization Application”). In the Naturalization Application, Kourani declared, among other things, that:

i. He had never “been a member of or in any way associated (*either directly or indirectly*) with . . . [a] terrorist organization.”

ii. He had never “given false or misleading information to any U.S. government official while applying for any immigration benefit”

iii. He had never “lied to any U.S. government official to gain entry or admission into the United States.”

d. On or about April 15, 2009, the Naturalization Application was approved, and Kourani became a naturalized citizen of the United States.

e. In or about April 2009, Kourani obtained a United States passport.

f. Based on passports used by Kourani and information from law enforcement databases, Kourani’s foreign travel has included the following:

i. On or about July 4, 2010, Kourani entered Lebanon. On or about August 17, 2010, Kourani returned to the United States.

ii. On or about June 23, 2011, Kourani entered Geneva, Switzerland; and on or about October 17, 2011, Kourani departed Lebanon (the “2011 Lebanon Trip”).

iii. On or about June 12, 2012, Kourani entered Lebanon.

iv. On or about July 13, 2012, Kourani entered Lebanon.

v. On or about December 26, 2012, Kourani entered Lebanon; and on or about January 12, 2013, Kourani exited Lebanon (the “2012 Lebanon Trip”).

g. In or about April 2013, Kourani obtained a United States passport card.

h. On or about September 18, 2015, when Kourani attempted to enter the United States at John F. Kennedy International Airport, law enforcement personnel identified a micro SD card secreted under a travel sticker affixed to Kourani's U.S. passport.¹

C. Kourani's 2016 Interviews with the FBI

7. Based on my participation in this investigation, I know that in or about 2016, Kourani was approached by United States authorities on several occasions. Based on my review of reports relating to those interviews, Kourani made the following statements, in substance and in part:

a. Kourani repeatedly denied membership in, or affiliation with, Hizballah.

b. Kourani's family name was akin to the "Bin Ladens of Lebanon."

c. Another one of Kourani's brothers, Qasem, had resided in the United States but later became a political leader and "face of Hizballah" in Yatar, Lebanon.

d. Husam Kourani, described by Kourani at various times during the interviews as a friend or cousin, was a member and "soldier" of Hizballah who moved to the United States, and then moved to Sao Paulo, Brazil in approximately 2005 after being approached by authorities in the United States.²

e. Muhammad Kourani (no relation) was the son of a former senior member of Hizballah known as Sheikh Hussein Kourani, and the husband of Kourani's sister, Layla Kourani.

¹ Law enforcement did not obtain the contents of the SD card.

² Records maintained by the Department of Homeland Security suggest that Husam Kourani took a commercial flight from the United States to Bogota, under an assumed name, on June 29, 2007.

f. Kourani was in Yater, Lebanon in 2006 when war broke out with Israel. *See* paragraph 5(f), *supra*. Kourani and certain of his relatives fled to Damascus, Syria, and then returned to New York. A home belonging to Kourani's father was destroyed in the conflict.

D. Kourani's 2017 Admissions to the FBI

8. In approximately March 2017, after an attorney (the "Attorney") contacted the FBI on behalf of Kourani and requested a meeting, Kourani participated in a series of interviews with FBI personnel. The Attorney was present during the interviews, and Kourani explained, in substance and in part, that he wished to provide information to the FBI in the hope of obtaining financial support as well as immigration benefits for certain of his relatives in Lebanon and Canada. No promises were made to Kourani regarding the availability of such benefits.

9. Based on my review of reports relating to interviews of Kourani beginning in approximately March 2017, as well as conversations with another FBI agent who participated in the interviews, I know that Kourani made the following statements, in substance and in part:

a. In approximately 2000, Kourani attended a 45-day Hizballah "boot camp" in Lebanon. Kourani was approximately 16 at the time, and he was permitted to attend because of his family's connections to a high-ranking Hizballah official named Haider Kourani. During the training, Kourani was taught to fire AK-47s and rocket launchers, as well as basic military tactics, by Hizballah personnel wearing uniforms.

b. Between approximately 2008 and approximately September 2015,³ Kourani was a member of the IJO, which is responsible for "black ops" on behalf of Hizballah and "the

³ In earlier interviews in 2017, Kourani stated, in substance and in part, that he was recruited to join IJO in approximately 2010. He subsequently corrected the date, to 2008, and explained that

Iranians.” By the time Kourani was a member of the IJO, and thereafter, he understood that Hassan Nasrallah, the Secretary General of Hizballah, operated IJO and reported directly to Ali Khamenei, the Supreme Leader of Iran.

c. Sheikh Hussein Kourani recruited Kourani to join the IJO in Lebanon in approximately 2008. During subsequent meetings in Lebanon with members or associates of Hizballah, Kourani was asked questions about his background and provided with training regarding, among other things, resisting interrogation. Kourani was also trained to gather and report on details about airport security, such as information relating to airport security personnel and the location of security cameras.

d. Following Kourani’s initial IJO training sessions, Kourani was taken to a meeting in Lebanon with a man named “Fadi” or “Hajj” (“Fadi”), who acted as Kourani’s handler while Kourani was a member of the IJO. Fadi told Kourani that he was expected to be operational within the United States, but could also be sent to another location or recalled to Lebanon if a war broke out.

e. One of Fadi’s initial taskings to Kourani was to identify and assess military and intelligence targets in the New York City area, as well as a source of firearms for Hizballah to cache weapons in the City. In response to that tasking, Kourani conducted surveillance, some of which he videotaped, of an armory facility on 27th Street in Manhattan between Fifth Avenue and

he had lied initially because he believed that the truthful information about his recruitment and membership in the organization could jeopardize his status as a naturalized citizen.

Park Avenue. Kourani also identified an FBI office in Manhattan and a Secret Service office in Brooklyn.⁴

f. In approximately 2011, Kourani returned to Lebanon after his initial mission. *See* paragraph 6(f)(ii), *supra* (describing an October 2011 exit from Lebanon). Kourani transported some of the products of his surveillance back to Lebanon on a micro SD card. *See* paragraph 6(h), *supra* (describing micro SD card secreted in Kourani's passport upon returning to the United States in September 2015).

g. In Lebanon, Kourani identified to a Hizballah handler other than Fadi the FBI office in Manhattan and the Secret Service office in Brooklyn. Kourani provided images from Google Earth of those buildings, as well as video of the armory facility in Manhattan. Kourani provided Fadi with approximately 10 telephone numbers of individuals Kourani believed could supply firearms in the future, but Fadi indicated that the contacts were not sufficiently reliable. Kourani also provided Fadi with information regarding John F. Kennedy International Airport, including the manner in which passengers disembark from planes, are screened at customs, and collect luggage, as well as the locations of security personnel, security cameras, and magnetometers.

⁴ During one of the interviews, Kourani confirmed by reviewing photographs that he had provided Fadi with surveillance information relating to 26 Federal Plaza (which includes FBI offices), the Army National Guard Building at 2366 5th Avenue in Manhattan, the U.S. Army 69th Regiment Armory at 68 Lexington Avenue in Manhattan, and the U.S. Secret Service Office Building at 335 Adams Street in Brooklyn.

h. In approximately July 2011, Kourani attended a Hizballah military training camp, located at Birkat Jabrur, Lebanon, where he was trained to use—and fired—several weapons (including AK-47s, MP-5 sub-machineguns, and grenade launchers).

i. During the 2011 Lebanon Trip, Kourani was tasked with purchasing equipment, such as drones, night-vision goggles, and high-powered cameras, so that Hizballah could work with Iranian or Russian associates to duplicate the technology. Kourani told the FBI, however, that he did not purchase any of these items.

j. Also during the 2011 Lebanon Trip, Sheikh Hussein Kourani told Kourani that he had just met with Mohammad Hamadi, a man Kourani described as a prominent member of Hizballah who had participated in the plot to hijack TWA flight 847, *see* paragraph 5(c), *supra*. Sheikh Hussein Kourani told Kourani that Hamadi still worked for Hizballah after serving a significant term of imprisonment in Germany, and should inspire Kourani to “man up.”

k. In approximately December 2012, while Kourani was in Lebanon, he spoke with Fadi about the July 2012 bombing in Bulgaria. *See* paragraph 6(f)(iii)-(v), *supra*. Fadi was critical of some aspects of the operation, and Kourani believed based on Fadi’s comments that he was involved in coordinating the attack.

l. In approximately 2012 or 2013, Fadi directed Kourani to obtain a U.S. passport card so that, in the event his U.S. passport was seized, he could use the passport card to transit the U.S. border. *See* paragraph 6(f)(iii)-(v), *supra* (describing multiple entries into Lebanon in 2012). Kourani confirmed that his April 2013 application for a U.S. passport card, *see* paragraph 6(g), *supra*, was submitted in response to this tasking from Fadi.

m. Kourani was trained to use digital storage media, such as memory cards, to transport pictures and data back to Lebanon. He was also trained to use email accounts to communicate regarding operational activities and to send information back to Lebanon. Kourani said that he used the email addresses, including ali.m.kourani@gmail.com and alikuku@hotmail.com, to communicate with Fadi using predetermined codes that they discussed in person. Kourani stated that he would regularly delete communications with Hizballah operatives, including his handlers, immediately upon reading them.

n. Kourani stated that he owns an Apple laptop and keeps it in his home, and that he used to own a Toshiba laptop, which was destroyed when his daughter spilled something on it. Kourani also stated that he used his cellular telephone and one or more laptop computers to access ali.m.kourani@gmail.com and alikuku@hotmail.com.

o. Fadi tasked Kourani with seeking information regarding the Israeli Consulate in New York City and Jewish businessmen in the area who were current or former members of the Israeli Defense Forces ("IDF"), especially those who were veterans of the 2006 War. Kourani understood that such individuals could be targeted by the IJO for either recruitment or assassination, and he said that he located people in New York associated with the IDF by searching the LinkedIn website using his account.

IV. The Subject Premises

10. On or about September 12, 2016, Kourani entered the United States after returning from Lebanon. Based on my review of the Customs Declaration that Kourani completed upon his return, I know that Kourani indicated that his "U.S. Street Address" was "183 W 238th St, 51W" in the Bronx, New York, *i.e.*, the Subject Premises.

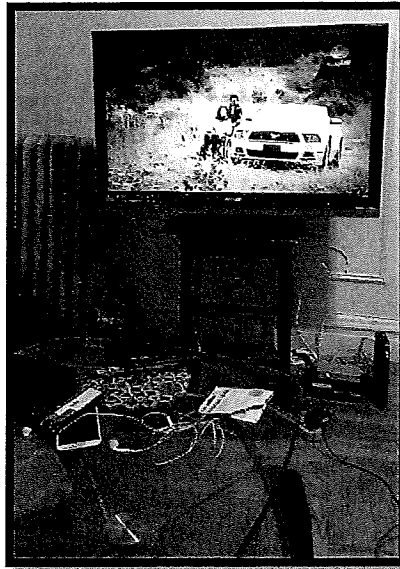
11. On or about May 11, 2017, the Honorable Gabriel W. Gorenstein, Magistrate Judge, issued a search warrant relating to the email account ali.m.kourani@gmail.com, *i.e.*, one of the email accounts that Kourani told the FBI he used for operational purposes, *see* paragraph 9(m), *supra*. Based on my review of materials provided by Google, Inc., in response to the search warrant, I know that:

a. On or about May 7, 2017, Kourani sent an email with subject line “Apartment for rent in kingsbridge,” signed “Best regards[,] Ali Kourani,” that stated: (i) that Kourani’s “Present Address” was 183 w 238 st apt 51w, Bronx NY 10453,” *i.e.*, the Subject Premises; and (ii) Kourani’s “Phone#” is 917-617-7039.

b. Between at least approximately May 20, 2016 and approximately May 9, 2017, there was a Samsung SM-G930T smartphone linked to Kourani’s email account, ali.m.kourani@gmail.com.

c. The user of an account linked to ali.m.kourani@gmail.com on a particular messaging application (“Application-1”), who appears to be Kourani, used Application-1 to send a series of photographs of what appear to be the Subject Premises. One of the photographs, which appears to have been sent by Kourani using Application-1 on or about February 3, 2017, depicts a white smartphone as well as a wireless router connected to a television⁵:

⁵ Even to the extent the photograph does not reflect the Subject Premises, I respectfully submit that the photograph also tends to suggest that Kourani has access to a smartphone that may be found within the Subject Premises.



12. On or about May 19, 2017, the Honorable Gabriel W. Gorenstein, Magistrate Judge, issued a warrant authorizing the FBI to obtain geolocation data relating to the cellular telephone assigned the phone number provided by Kourani in the above-described May 7, 2017 email (917-617-7039), *see* paragraph 11(a), *supra*. Based on my review of data provided in response to the May 19, 2017 warrant, I know that, at least once between 7:00 p.m. and 8:00 a.m., on each day between on or about May 19 and on or about May 22, 2017, the device associated with 917-617-7039 has been located within seven meters or less of the street address associated with the Subject Premises.

13. Based on my training and experience, I know that individuals such as Kourani who are engaged in unlawful activities with and on behalf of foreign actors often safekeep documents and electronic devices related to these activities at their homes, such as the Subject Premises. This is particularly true under circumstances such as those here, where Kourani has admitted that he used electronic storage media to transport information back to Lebanon, and that he keeps a laptop in

his home, *see* paragraphs 9(m)-9(n), *supra*.

14. Based on my training, experience, and participation in this and related investigations, I know that:

a. Individuals engaged in the Subject Offenses often use computers, phones, and other electronic devices to, among other things, communicate with co-conspirators, store surveillance and intelligence data, arrange travel, and keep a record of transactions and foreign trips. In my training and experience, I know that people who have extensive overseas contacts are even more likely to utilize internet-based devices and applications to communicate with their contacts, such as email, voice-over-internet protocols, and messaging applications (such as Application-1). Evidence obtained pursuant to a search warrant relating to the email account ali.m.kourani@gmail.com corroborates Kourani's statements to the FBI indicating that he has used Application-1 to communicate with people he described as members or associates of Hizballah. I also know that Kourani has used electronic media to store and transport information relating to his criminal activities, as described in paragraph 9(m), *supra*. As a result, individuals such as Kourani often store data on their computers related to their criminal activities, which can include logs of online chats, emails, contact information of co-conspirators, including telephone numbers, email addresses, and identifiers for instant messaging and social media accounts, and personal financial information.

b. Electronic files can be stored on a hard drive or cellphone for years at little to no cost and users thus have little incentive to delete data that may have useful to consult in the future.

c. Computer files or remnants of such files can be recovered months or even years after they have been created or saved on an electronic device such as the cellphone apparently used by Kourani. Even when such files have been deleted, they can often be recovered, depending on how the hard drive has subsequently been used, months or years later with forensics tools. Thus, the ability to retrieve from information from electronic devices depends less on when the information was first created or saved than on a particular user's device configuration, storage capacity, and computer habits.

d. Even when a user does choose to delete data, that data can often be recovered months or years later with the appropriate forensic tools. When a file is "deleted" on a home computer, the data contained in the file does not actually disappear, but instead remains on the hard drive, in "slack space," until it is overwritten by new data that cannot be stored elsewhere on the computer. Similarly, the files that have been viewed on the Internet are generally downloaded into a temporary Internet directory or "cache," which is only overwritten as the "cache" fills up and is replaced with more recently viewed Internet pages. Thus, the ability to retrieve from a hard drive or other electronic storage media depends less on when the file was created or viewed than on a particular user's operating system, storage capacity, and computer habits.

e. In the event that a user changes computers, the user will typically transfer files from the old computer to the new computer, so as not to lose data. In addition, users often keep backups of their data on electronic storage media such as thumb drives, flash drives, memory cards, CD-ROMs, or portable hard drives.

15. Based on my training, experience, and participation in this investigation, with respect

to computer and electronically-stored data, I also know that:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media,⁶ and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence relating to the “who, what, why, when, where, and how” of the Subject Offenses, thus enabling the Government to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media commonly includes “user attribution evidence,” such as registry information, communications, images and movies, transactional information, records of

⁶ The term “storage media” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

session times and durations, internet history, as well as anti-virus, spyware, and malware detection programs, which can indicate who has used or controlled the computer or storage media.

c. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the Subject Offenses.

d. Some information stored within a computer or electronic storage media may provide evidence relating to the physical location of other evidence, all of targets of the investigation or their associates. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user.

e. Some information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example,

information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

f. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when they did so.

g. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

16. Based on the foregoing, I respectfully submit that there is probable cause to believe that Kourani and others are engaged in the Subject Offenses, and that evidence of this criminal activity, which is described in Attachment A, is likely to be found in the Subject Premises and on computers,⁷ electronic devices, and electronic storage media found in the Subject Premises,

⁷ The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

including:

a. Records and information⁸ concerning occupancy or ownership of the Subject Premises, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys;

b. Records and information relating to travel in furtherance of the Subject Offenses;

c. Records and information—including books, records, invoices, receipts, records of real estate transactions, bank statements and related records, passbooks, money drafts, letters of credit, cashier's checks, bank checks, safe deposit box keys, money wrappers, and other items evidencing the obtaining, secreting, transfer and/or the concealment of assets and the obtaining, secreting, transfer, concealment and/or the expenditure of money—relating to financial transactions in furtherance of the Subject Offenses, including records and information relating to funds transfers to and from Lebanon as well as subsequent disbursements of those funds;

d. Records and information relating to communications in furtherance of the Subject Offenses, such as (i) communications and online postings relating to the Subject Offenses, including communications relating to the provision of support to Hizballah, the receipt of military-type training from Hizballah, taskings on behalf of Hizballah, surveillance conducted for Hizballah, the use and acquisition of weapons, and the making of false statements to the U.S. government; (ii) communications and online postings related to purchases or efforts to acquire weapons, bomb components, and/or chemical precursors for bombs; and (iii) communications and online postings pertaining in any way to Hizballah or other terrorist organizations;

e. Records and information relating to purchases or efforts to acquire weapons, bomb components, and/or chemical precursors for bombs;

f. Records and information relating to the acquisition of U.S. travel documents or visas for travel to countries outside of the United States in furtherance of the Subject Offenses; and

g. Records and information relating to Hizballah's structure, membership, objectives, or other activities, including but not limited to evidence of Hizballah's designation as

⁸ The terms "records" and "information" include all forms of creation or storage, including any form of computer or electronic storage (such as hard drives or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

a foreign terrorist organization, and the fact that Hizballah engages in or has engaged in terrorist activities.

V. Procedures for Searching Electronically Stored Information (“ESI”)

A. Execution of Warrant for ESI

17. Federal Rule of Criminal Procedure 41(e)(2)(B) provides that a warrant to search for and seize property “may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information . . . for later review.” Consistent with Rule 41, this application requests authorization to seize any computer device and electronic storage media and transport them to an appropriate law enforcement facility for review. This is typically necessary for a number of reasons:

- First, the volume of data on computer devices and storage media is often impractical for law enforcement personnel to review in its entirety at the search location.
- Second, because computer data is particularly vulnerable to inadvertent or intentional modification or destruction, computer devices are ideally examined in a controlled environment, such as a law enforcement laboratory, where trained personnel, using specialized software, can make a forensic copy of the storage media that can be subsequently reviewed in a manner that does not change the underlying data.
- Third, there are so many types of computer hardware and software in use today that it can be impossible to bring to the search site all of the necessary technical manuals and specialized personnel and equipment potentially required to safely access the underlying computer data.
- Fourth, many factors can complicate and prolong recovery of data from a computer device, including the increasingly common use of passwords, encryption, or other features or configurations designed to protect or conceal data on the computer, which often take considerable time and resources for forensic personnel to detect and resolve.

B. Review of Electronic Evidence

18. Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (including, in addition to law enforcement

officers and agents, and depending on the nature of the electronic evidence and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained therein for information responsive to the warrant.

19. In conducting this review, law enforcement personnel may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- conducting a file-by-file review by “opening” or reading the first few “pages” of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- “scanning” storage areas to discover and possibly recover recently deleted data or deliberately hidden files; and
- performing electronic keyword searches through all electronic storage areas to determine the existence and location of data potentially related to the subject matter of the investigation⁹; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

20. Law enforcement personnel will make reasonable efforts to restrict their search to data

⁹ Keyword searches alone are typically inadequate to detect all relevant data. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.

falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement personnel may need to conduct a complete review of all the ESI from seized devices or storage media to evaluate its contents and to locate all data responsive to the warrant.

C. Return of ESI

21. If the Government determines that the electronic devices are no longer necessary to retrieve and preserve the data, and the devices themselves are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return these items, upon request. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.

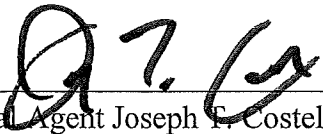
VI. Request to Search the Subject Premises and Items to be Seized

22. Based on my training, experience, participation in this and other investigations, I know that individuals who participate in criminal activities, including the Subject Offenses, routinely secrete and store books, records, documents, currency and other items of the sort described in each Attachment A in secure locations like safety deposit boxes, suitcases, safes, key-lock strong boxes, and other types of locked or closed containers or rooms in an effort to prevent the discovery or theft of said items. The requested warrant and search procedure includes a search of any closed containers on the Subject Premises, including cabinets, closets, doors to rooms, and other appurtenances located on or within the Subject Premises whether they are locked or unlocked.


23. Based on the foregoing, I respectfully submit that there is probable cause to believe that the Subject Premises have been and are continuing to be used to store instrumentalities, evidence, and fruits of the Subject Offenses, as described in Attachment A to the proposed warrant.

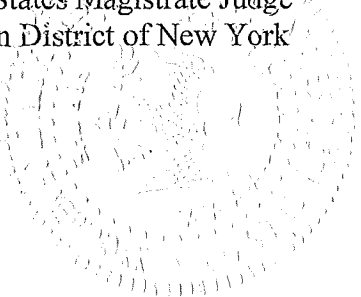
24. Based on the foregoing, I respectfully request the court to issue the requested warrant to seize the items and information specified in each Attachment A to this affidavit and to the Search and Seizure Warrant.

25. In light of the confidential nature of the continuing investigation, including because the investigation is not known to all of the targets of the investigation, I respectfully request that this Affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise.


Special Agent Joseph P. Costello
Federal Bureau of Investigation

Sworn to before me this
31st Day of May, 2017


HONORABLE KATHARINE H. PARKER
United States Magistrate Judge
Southern District of New York



Attachment A

I. Property to be Searched

The entire premises, including all closed and locked containers, closets, and rooms at the premises located at 183 West 238 Street, Apartment 51W, Bronx, New York 10463 (the "Subject Premises"), which is an apartment in a multi-story apartment building that appears from the outside as follows:



II. Items to be Seized

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be seized from the Subject Premises include the following evidence, fruits, and instrumentalities of violations of (i) Title 18, United States Code, Section 2339B (providing and conspiracy to provide material support or resources to designated foreign terrorist organizations); (ii) Title 18, United States Code, Sections 2339D and 371 (receipt of, and conspiracy to receive, military-type training from designated foreign terrorist organizations); (iii) Title 18, United States Code, Section 924 (firearms offenses related to crimes of violence); (iv) Title 18, United States Code, Section 1001 (making false statements or omissions in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States); and (v) Title 18, United States Code, Section 1425 (procurement of citizenship or naturalization unlawfully) (the "Subject Offenses"), including:

a. Records and information¹ concerning occupancy or ownership of the Subject Premises, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys;

¹ The terms "records" and "information" include all forms of creation or storage, including any form of computer or electronic storage (such as hard drives or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

b. Records and information relating to travel in furtherance of the Subject Offenses;

c. Records and information—including books, records, invoices, receipts, records of real estate transactions, bank statements and related records, passbooks, money drafts, letters of credit, cashier's checks, bank checks, safe deposit box keys, money wrappers, and other items evidencing the obtaining, secreting, transfer and/or the concealment of assets and the obtaining, secreting, transfer, concealment and/or the expenditure of money—relating to financial transactions in furtherance of the Subject Offenses, including records and information relating to funds transfers to and from Lebanon as well as subsequent disbursements of those funds;

d. Records and information relating to communications in furtherance of the Subject Offenses, such as (i) communications and online postings relating to the Subject Offenses, including communications relating to the provision of support to Hizballah, the receipt of military-type training from Hizballah, taskings on behalf of Hizballah, surveillance conducted for Hizballah, the use and acquisition of weapons, and the making of false statements to the U.S. government; (ii) communications and online postings related to purchases or efforts to acquire weapons, bomb components, and/or chemical precursors for bombs; and (iii) communications and online postings pertaining in any way to Hizballah or other terrorist organizations;

e. Records and information relating to purchases or efforts to acquire weapons, bomb components, and/or chemical precursors for bombs;

f. Records and information relating to the acquisition of U.S. travel documents or visas for travel to countries outside of the United States in furtherance of the Subject Offenses; and

g. Records and information relating to Hizballah's structure, membership, objectives, or other activities, including but not limited to evidence of Hizballah's designation as a foreign terrorist organization, and the fact that Hizballah engages in or has engaged in terrorist activities.

B. Search and Seizure of Electronically Stored Information ("ESI")

The items to be seized from the Subject Premises also include any computer devices and storage media that may contain any electronically stored information falling within the categories set forth in Section II.A of this Attachment above, including, but not limited to, desktop and laptop computers, disk drives, modems, thumb drives, personal digital assistants, smart phones, digital cameras, and scanners, as well as routers, modems, and network equipment used to connect to the Internet. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

The items to be seized from the Subject Premises also include:

1. Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.

2. Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.

3. Any evidence concerning the persons with access to, control over, or ownership of the seized or copied computer devices or storage media.

C. Review of ESI

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (which may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Section II of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

AO 93 (SDNY Rev. 01/17) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
Southern District of New YorkIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

See Attachment A

Case No.

17 MAG 4152

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Southern District of New York
(identify the person or describe the property to be searched and give its location):

See Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

See Attachment A

The search and seizure are related to violation(s) of (insert statutory citations):

See Attachment A, Subject Offenses

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before

6-13-17

(not to exceed 14 days)

- ☐
- in the daytime 6:00 a.m. to 10 p.m.
- ☒
- at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Clerk of the Court.

- ☐
- Upon its return, this warrant and inventory should be filed under seal by the Clerk of the Court.

USMJ Initials

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30).☐ until, the facts justifying, the later specific date of _____.

Date and time issued:

5-31-17
7:45 p.m.Katharine H. Parker
Judge's signatureCity and state: New York, NY

Hon. Katharine H. Parker, USMJ, SDNY

Printed name and title

Attachment A

I. Property to be Searched

The entire premises, including all closed and locked containers, closets, and rooms at the premises located at 183 West 238 Street, Apartment 51W, Bronx, New York 10463 (the “Subject Premises”), which is an apartment in a multi-story apartment building that appears from the outside as follows:



II. Items to be Seized

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be seized from the Subject Premises include the following evidence, fruits, and instrumentalities of violations of (i) Title 18, United States Code, Section 2339B (providing and conspiracy to provide material support or resources to designated foreign terrorist organizations); (ii) Title 18, United States Code, Sections 2339D and 371 (receipt of, and conspiracy to receive, military-type training from designated foreign terrorist organizations); (iii) Title 18, United States Code, Section 924 (firearms offenses related to crimes of violence); (iv) Title 18, United States Code, Section 1001 (making false statements or omissions in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States); and (v) Title 18, United States Code, Section 1425 (procurement of citizenship or naturalization unlawfully) (the “Subject Offenses”), including:

a. Records and information¹ concerning occupancy or ownership of the Subject Premises, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys;

¹ The terms “records” and “information” include all forms of creation or storage, including any form of computer or electronic storage (such as hard drives or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

b. Records and information relating to travel in furtherance of the Subject Offenses;

c. Records and information—including books, records, invoices, receipts, records of real estate transactions, bank statements and related records, passbooks, money drafts, letters of credit, cashier's checks, bank checks, safe deposit box keys, money wrappers, and other items evidencing the obtaining, secreting, transfer and/or the concealment of assets and the obtaining, secreting, transfer, concealment and/or the expenditure of money—relating to financial transactions in furtherance of the Subject Offenses, including records and information relating to funds transfers to and from Lebanon as well as subsequent disbursements of those funds;

d. Records and information relating to communications in furtherance of the Subject Offenses, such as (i) communications and online postings relating to the Subject Offenses, including communications relating to the provision of support to Hizballah, the receipt of military-type training from Hizballah, taskings on behalf of Hizballah, surveillance conducted for Hizballah, the use and acquisition of weapons, and the making of false statements to the U.S. government; (ii) communications and online postings related to purchases or efforts to acquire weapons, bomb components, and/or chemical precursors for bombs; and (iii) communications and online postings pertaining in any way to Hizballah or other terrorist organizations;

e. Records and information relating to purchases or efforts to acquire weapons, bomb components, and/or chemical precursors for bombs;

f. Records and information relating to the acquisition of U.S. travel documents or visas for travel to countries outside of the United States in furtherance of the Subject Offenses; and

g. Records and information relating to Hizballah's structure, membership, objectives, or other activities, including but not limited to evidence of Hizballah's designation as a foreign terrorist organization, and the fact that Hizballah engages in or has engaged in terrorist activities.

B. Search and Seizure of Electronically Stored Information ("ESI")

The items to be seized from the Subject Premises also include any computer devices and storage media that may contain any electronically stored information falling within the categories set forth in Section II.A of this Attachment above, including, but not limited to, desktop and laptop computers, disk drives, modems, thumb drives, personal digital assistants, smart phones, digital cameras, and scanners, as well as routers, modems, and network equipment used to connect to the Internet. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

The items to be seized from the Subject Premises also include:

1. Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.

2. Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.

3. Any evidence concerning the persons with access to, control over, or ownership of the seized or copied computer devices or storage media.

C. Review of ESI

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (which may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Section II of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

AO 93 (SDNY Rev. 01/17) Search and Seizure Warrant (Page 2)

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the Court.

Date: _____

Executing officer's signature

Printed name and title